PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-077129**
(43)Date of publication of application : **15.03.2002**

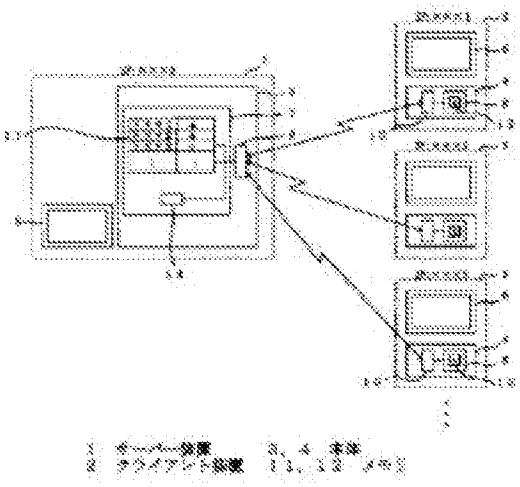
(51)Int.Cl. H04L 9/08
G06F 15/00

(21)Application number : **2000-253214**
(22)Date of filing : **24.08.2000**

(71)Applicant : **NISSIN ELECTRIC CO LTD**
(72)Inventor : **FUJIMURA SHIGERU**

(54) METHOD OF COMMUNICATING ENCRYPTION

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate a burden such as the determination, control or the like of a key code for coding and decoding of a user for a client device, and to improve security by coding transmit-receive information after a previous time before the completion of a log-in and to enhance reliability on communication in client-server type telecommunication.
SOLUTION: When the client device 2 is logged into a server device 1 and communication is conducted between the server device 1 and the client device 2, the key codes for coding and decoding of the client device 2 are registered previously in the server device 1 in response to the address or terminal name of the client device 2 while being set in the client device 2, a series of transmit- receive information between the server device 1 and the client device 2 after the log-in demand of the client device 2 is coded on the basis of the key codes by the transmit-receive processing of the server device 1 and the client device 2, and reception information is decoded on the basis of the key codes.



CLAIMS

[Claim(s)]
[Claim 1]When a client apparatus logs in to a server system and it communicates between said server system and said client apparatus, While making an address or a terminal name of said client apparatus correspond beforehand and registering a key code of dark and a decoding of said client apparatus into said server system, Set it as said client apparatus and by transmitting and receiving processing of said server system and said client apparatus. A cipher communication method enciphering a series of transmit information between said server system after a login request of said client apparatus, and said client apparatus based on said key code, and decoding receipt information based on said key code.
[Claim 2]Based on a connection request before a login request of said client apparatus, for every login of a client apparatus, Said server system determines a key code of dark and a decoding, and this key code, The cipher communication method according to claim 1 transmitting and setting it as said client apparatus while registering with said server system, and updating said key code of said server system and said client apparatus with said server system for every login of said client apparatus.
[Claim 3]The cipher communication method according to claim 1 or 2, wherein communication between a server system and a client apparatus is performed on radio.
DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the cipher communication method between the server system of what is called a client server type of information and telecommunications, and a client apparatus.
[0002]
[Description of the Prior Art]If it is in the database system etc. of the client server type built by LAN etc. conventionally, two or more client apparatus log in to a server system, and communication is performed between a server system and each client apparatus.
[0003]And when all or a part of these communications are radio-ized and what is called wireless LAN etc. are built, The wireless communication means of the cellular phone which contains a short form (PHS) in a server system and each client apparatus, an operating walkie-talkie, etc. is attached, and radio is performed by these wireless communication means between a server system and each client apparatus through an electric wave.
[0004]On the other hand, when each client apparatus logs in to a server system, each client apparatus Each address. A password and user ID need to be accounted, especially, a server system attests each client apparatus with the password of this account, and login is completed. Then, information is actually exchanged between a server system and each client apparatus.

[0005]
[Problem to be solved by the invention]Even if communication of the cable between said server

system and each client apparatus or radio is any of analog communication and Digital Communications Division, the communications protocol is exhibited.
[0006]Therefore, the information exchanged between a server system and each client apparatus has the high danger of embezzling for a third party, by using the communication equipment etc. which suited this protocol.
[0007]Then, communication between a server system and each client apparatus is enciphered, and it is possible to aim at improvement in the confidentiality and reliability.
[0008]And although there is a common key encryption system using the key code of the same dark and decoding in the public-key crypto system etc. from which the key code of dark and a decoding differs by encryption and decoding, and encryption and a decoding conventionally as a cipher system of this communication, While all determine a key code and the user (user) of each client apparatus itself sets them as each client apparatus, respectively, it is necessary to notify and register with a server system.
[0009]Therefore, if it is in the conventional encryption communication, to the user of each client apparatus. There is a problem to which great burdens, such as determination of the key code of each dark and decoding and management, are applied, and if a key code is changed for every login and it tries to aim at much more improvement in confidentiality and reliability especially, the burden of the user of each client apparatus will increase further.
[0010]And in the case of said conventional encryption communication, only the information exchanged after the completion of login is enciphered, It is not enciphered but a login request, a password, etc. which are transmitted and received before the completion of login have a possibility that these may be used by stealth for a third party, and especially when they communicate on radio, they also have the problem that the danger is very high.
[0011]This invention loses the burden of the determination for every login of the key code of the dark and decoding of the user of each client apparatus, management, etc., moreover, enciphers transmission-and-reception information from before the completion of login, improves confidentiality, and makes it SUBJECT to improve communicative reliability.
[0012]
[Means for solving problem]In order to solve aforementioned SUBJECT, the cipher communication method of this invention, When in the case of Claim 1 a client apparatus logs in to a server system and it communicates between a server system and a client apparatus, While making the address or terminal name of a client apparatus correspond beforehand and registering the key code of the dark and decoding of a client apparatus into a server system, It is set as a client apparatus, and by the transmitting and receiving processing of a server system and a client apparatus, a series of transmit information between the server system after the login request of a client apparatus and a client apparatus is enciphered based on a key code, and receipt information is decoded based on a key code.
[0013]Therefore, while a key code of dark and a decoding of a client apparatus is beforehand registered into a server system, it is set as a client apparatus, determination for every login of a key code of dark and a decoding by a user of a client apparatus, management, etc. are

unnecessary, and the burden is eased.
[0014]And since all information exchanged between a server system after a login request of a client apparatus and a client apparatus is enciphered based on a key code of dark and a decoding registered and set up beforehand, Information is enciphered from before the completion of login, confidentiality is very high and communicative reliability improves remarkably.
[0015]Next, in the case of Claim 2, based on a connection request before a login request of a client apparatus for every login of a client apparatus, A server system determines a key code of dark and a decoding, while registering this key code into a server system, it is transmitted and set as a client apparatus, and a key code of a server system and a client apparatus is updated with a server system for every login of a client apparatus.
[0016]Therefore, confidentiality improves further, without being set as a client apparatus, being updated and applying a burden to a user of a client apparatus for every login of a client apparatus, while a key code of dark and a decoding is automatically registered into a server system by a server system.
[0017]And the cipher communication method of this invention is very preferred when there are many opportunities of use of communication between a server system and a client apparatus of **** and a third party by radio.
[0018]
[Mode for carrying out the invention]It explains with reference to drawing 1 per form of enforcement of this invention - drawing 3. Drawing 1 shows one example of the telecommunications system of the client server type built by wireless LAN, Two or more client apparatus 2 which log in to the server system 1 and this server system 1 as a database server, It has the main parts 3 and 4 and the monitor display devices 5 and 6 which were formed with the microcomputer etc., respectively, and the main parts 3 and 4 are provided with the wireless radios 9 and 10, such as the sending and receiving processors 7 and 8 and a cellular phone, or an operating walkie-talkie.
[0019]As for the server system 1 and each client apparatus 2, addresses, such as an IP address, are set up, and account of user ID, such as a terminal name, and a password is given to each client apparatus 2.
[0020]Next, the key code of the dark and decoding of each client apparatus 2 consists of a code common to an encryption key and a decode key or a code of an encryption key, and a code of a decode key.
[0021]And in order to explain simply, an IP address is set as the server system 1 and each client apparatus 2, When the address is made into xxx0, xxx1, xxx2, xxx3, and -- and the key code of the dark and decoding of each client apparatus 2 is made into a, b, c, d, and --, these key codes, First, the administrator of LAN determines, and the IP address or terminal name of each client apparatus 2 is made to correspond to the nonvolatile memory 11 in which rewriting as a key code registration table provided in the sending and receiving processor 7 of the server system 1 is free, and it writes in and registers with it.
[0022]Each first key code is written in and set as the rewritable nonvolatile memory 12 provided

in the sending and receiving processor 8 of each client apparatus 2 by setting out of the user of each client apparatus based on said administrator's setting out or mailing etc.
[0023]Thus, while the key code of dark and a decoding was registered into the server system 1, after being set as the client apparatus 2, The server system 1 executes the server side transmitting-and-receiving-processing program of step A_1 of drawing 2 set as the main part 3 - A_{18}, and each client apparatus 2 executes the client side transmitting-and-receiving-processing program of step B_1 of drawing 3 set as those main parts 4 - B_{19}.
[0024]When the client apparatus 2 logs in to the server system 1 by execution of these programs, the client apparatus 2 carries out wireless transmission of the connection request to the server system 1 from the wireless radios 10 with the address by step B_1 and B_2 first.
[0025]And in order to determine and update the key code of dark and a decoding with the server system 1 for every login in this form, The server system 1 which received the connection request performs step A_4 via step A_1, A_2, and A_3, by the key code generation part 13 of the sending and receiving processor 7, generates the new key code which consists of a number and character set doubling, for example by the technique of a random number generation, and determines it.
[0026]Perform step A_5 and the determined key code is enciphered based on the key code registered [of the memory 11 corresponding to the address of the connection request], Wireless transmission is carried out from the wireless radios 9 with the address of the client apparatus 2, and after that, by step A_6, it rewrites to the new key code which determined the contents of registration of the memory 11, and updates automatically.
[0027]On the other hand, the client apparatus 2 which transmitted the connection request by step B_3 of drawing 2, B_4, and B_5. Receipt information is decoded based on the key code set [of the memory 12] up, the new key code which received from the server system 1 is written in the memory 12, and the key code is updated automatically.
[0028]And a login request is enciphered after renewal of this key code based on the key code of the memory 12 by step B_6 and B_7, and wireless transmission of the enciphered login request is carried out to the server system 1 with that address.
[0029]by step A_7 of drawing 2, decode receipt information based on the key code to which the memory 11 corresponds, and the server system 1 which received this wireless transmission should step A_8 boil it, if reception of the Lilo Guynn demand is detected, It enciphers based on the key code to which the memory 11 corresponds a password demand by step A_9 and A_{10}, and wireless transmission is carried out with an address.
[0030]That client apparatus 2 that received this wireless transmission, If receipt information is decoded based on the key code of the memory 12 via step B_8 by step B_9 and reception of a password demand is detected, Via step B_{10}, by step B_{11}, B_{12}, and B_{13}, it enciphers based on the key code of the memory 12, and wireless transmission of the password is carried out to the server system 1 with the address.
[0031]The server system 1 which received this wireless transmission is decoded by step A_7 of drawing 2, A password received by step A_{12} via step A_8 and A_{11} is identified (attestation), If it is the registered right password, a notice of allowance of login of the client apparatus 2 will be

published, a login notice of allowance is enciphered by step A_{13} and A_{14}, and wireless transmission is carried out.

[0032]If a password is not right, request sending is enciphered by step A_{15}, and wireless transmission is carried out to the client apparatus 2.

[0033]If the client apparatus 2 decodes receipt information by step B_9 of drawing 3 and step B_{14} detects reception of a login notice of allowance via step B_{10}, Step B_{15} performs encryption of transmit information based on a password of the memory 12, and a decoding of receipt information, and information is exchanged by the server system 1 and radio until it distinguishes the completion of login and logs out henceforth.

[0034]When reception of a login notice of allowance is undetectable by step B_{14}, request sending is enciphered to the server system 1 by step B_{16} and B_{17}, and it transmits.

[0035]When ending the exchange of the information on the server system 1, it shifts to step B_{19} via step $B_{18}$from step B15 , the notice of logout is enciphered, and wireless transmission is carried out to the server system 1.

[0036]On the other hand, by reception after a login notice of allowance, the server system 1 shifts to step $A_{16}$of drawing 2from step A2 , during login, decodes receipt information by step A_{16} based on the key code to which the memory 11 corresponds, and enciphers transmit information.

[0037]If the notice of logout is received, it will shift to step A_{18} via step $A_{17}$from step A16 , and logout processing will be performed.

[0038]And the process of the server system 1 at the time of logging in and the client apparatus 2 comes to be shown in the next table 1, and all the information after the login request exchanged between the server system 1 and the client apparatus 2 is enciphered by the key code so that clearly also from this table 1.

[0039]

[Table 1]

[0040]The numbers 1-27 of the head of each line of Table 1 are operation numbers, and * shows dark and decoding processing. After distinguishing the completion of login by the process 27 of Table 1, the information enciphered based on the key code between the server system 1 and the client apparatus 2 is exchanged.

[0041]Therefore, it is necessary to determine, the user of each client apparatus 2 does not need to manage the key code of each dark and decoding, and there are very few those users' burdens.

[0042]In order to encipher all the information after a login request by a key code and to carry out, the confidentiality of the information on a password etc. is very high, and communicative reliability improves remarkably.

[0043]And without applying a burden to the user of each client apparatus 2, in order to update automatically the key code of the server system 1 and each client apparatus 2 with the server system 1 for every login, confidentiality can be improved further and communicative reliability improves further.

[0044]Therefore, the very suitable cipher communication method for wireless LAN higher than the case where the danger of surreptitious use of a password etc. is a cable (on-line) etc. can be provided.
[0045]in order to improve confidentiality further -- the password of each client apparatus 2 -- yes, it is preferred to use a **** one-time password.
[0046]It enciphers with other cipher systems, such as what is called a public-key-encryption-ized system, instead of registered **** for key codes, and may be made to transmit and receive the coding information of a key code transmitted to the client apparatus 2 from the server system 1 to it in the case of renewal of the key code for every login.
[0047]Next, those terminal names are made to correspond instead of the address of each client apparatus 2, and the key code of each client apparatus 2 may be written in the memory 11, and, of course [when registering the key code of each client apparatus 2 into the server system 1], may be registered.
[0048]When attaining simplification of processing, etc., the key code for every login is not updated, The key code of the dark and decoding of each client apparatus 2 is registered and set only once as the server system 1 and each client apparatus 2 by an administrator etc. at the beginning, The information for every login is enciphered by this key code, it may be made to transmit and receive, and processing of step A_3-A_6 of drawing 2, step B_1 of drawing 3 - B_5 can be excluded in this case.
[0049]And this invention is applicable to various information and telecommunications which exchange the information between the server system 1 and each client apparatus 2 with radio or a cable.
[0050]
[Effect of the Invention]This invention does so the effect indicated below. First, in the case of Claim 1, the key code of the dark and decoding of the client apparatus 2, The information which is set as the client apparatus 2 while registering with the server system 1 beforehand, and is exchanged between the server system 1 and the client apparatus 2 based on the key code automatically Dark, since it is decrypted, The determination of the key code of the dark and decoding by the user of the client apparatus 2, management, etc. are unnecessary, the burden can be eased and encryption communication can be performed.
[0051]And since all the information exchanged between the server system 1 after the login request of the client apparatus 2 and the client apparatus 2 is enciphered based on the key code of the dark and decoding registered and set up beforehand, Information can be enciphered from before the completion of login, confidentiality can be made very high, and communicative reliability can be improved remarkably.
[0052]Next, without applying a burden to the user of the client apparatus 2, since the server system 1 determined the key code of dark and a decoding automatically and it was updated for every login of the client apparatus 2, in the case of Claim 2, confidentiality can be improved further, and it can improve communicative reliability further.
[0053]Since it applied when communication between the server system 1 and the client

apparatus 2 was performed on radio, when it is radio with the high danger of surreptitious use of a password etc., in the case of Claim 3, confidentiality can be improved further, and it can improve communicative reliability remarkably.